

AMENDED IN ASSEMBLY SEPTEMBER 1, 2015

AMENDED IN ASSEMBLY JULY 2, 2015

AMENDED IN SENATE MAY 21, 2015

AMENDED IN SENATE APRIL 6, 2015

**SENATE BILL**

**No. 570**

---

---

**Introduced by Senator Jackson**

February 26, 2015

---

---

An act to amend Sections 1798.29 and 1798.82 of the Civil Code, relating to personal information.

LEGISLATIVE COUNSEL'S DIGEST

SB 570, as amended, Jackson. Personal information: privacy: breach.

Existing law requires a person or business conducting business in California and any agency, as defined, that owns or licenses computerized data that includes personal information, as defined, to disclose a breach of the security of the system in the most expedient time possible and without unreasonable delay, as specified. Existing law requires a person, business, or agency that is required to issue a security breach notification to meet specific requirements, including that the notification be written in plain language.

This bill would additionally require the security breach notification to be titled "Notice of Data Breach" and to present the information under prescribed headings. The bill would prescribe a model security breach notification form, as specified.

*This bill would incorporate additional changes to Section 1798.29 of the Civil Code proposed by SB 34 and AB 964, that would become operative if this bill and one or both of those bills are enacted and this bill is chaptered last.*

*This bill also would incorporate additional changes to Section 1798.82 of the Civil Code proposed by SB 34 and AB 964, that would become operative if this bill and one or both of those bills are enacted and this bill is enacted last.*

Vote: majority. Appropriation: no. Fiscal committee: yes.  
State-mandated local program: no.

*The people of the State of California do enact as follows:*

1     SECTION 1. Section 1798.29 of the Civil Code is amended  
2     to read:  
3     1798.29. (a) Any agency that owns or licenses computerized  
4     data that includes personal information shall disclose any breach  
5     of the security of the system following discovery or notification  
6     of the breach in the security of the data to any resident of California  
7     whose unencrypted personal information was, or is reasonably  
8     believed to have been, acquired by an unauthorized person. The  
9     disclosure shall be made in the most expedient time possible and  
10    without unreasonable delay, consistent with the legitimate needs  
11    of law enforcement, as provided in subdivision (c), or any measures  
12    necessary to determine the scope of the breach and restore the  
13    reasonable integrity of the data system.  
14    (b) Any agency that maintains computerized data that includes  
15    personal information that the agency does not own shall notify the  
16    owner or licensee of the information of any breach of the security  
17    of the data immediately following discovery, if the personal  
18    information was, or is reasonably believed to have been, acquired  
19    by an unauthorized person.  
20    (c) The notification required by this section may be delayed if  
21    a law enforcement agency determines that the notification will  
22    impede a criminal investigation. The notification required by this  
23    section shall be made after the law enforcement agency determines  
24    that it will not compromise the investigation.  
25    (d) Any agency that is required to issue a security breach  
26    notification pursuant to this section shall meet all of the following  
27    requirements:  
28    (1) The security breach notification shall be written in plain  
29    language, shall be titled "Notice of Data Breach," and shall present  
30    the information described in paragraph (2) under the following  
31    headings: "What Happened," "What Information Was Involved,"

“What We Are Doing,” “What You Can Do,” and “For More Information.” Additional information may be provided as a supplement to the notice.

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		

1		
2	What You Can Do.	
3		
4		
5		
6		
7		
8		
9	Other Important Information.	
10	[insert other important information]	
11		
12		
13		
14		
15		
16		
17		
18	For More Information.	Call [telephone number] or go to [Internet Web site]
19		
20		
21		
22		

(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

1 (D) Whether the notification was delayed as a result of a law  
2 enforcement investigation, if that information is possible to  
3 determine at the time the notice is provided.

4 (E) A general description of the breach incident, if that  
5 information is possible to determine at the time the notice is  
6 provided.

7 (F) The toll-free telephone numbers and addresses of the major  
8 credit reporting agencies, if the breach exposed a social security  
9 number or a driver's license or California identification card  
10 number.

11 (3) At the discretion of the agency, the security breach  
12 notification may also include any of the following:

13 (A) Information about what the agency has done to protect  
14 individuals whose information has been breached.

15 (B) Advice on steps that the person whose information has been  
16 breached may take to protect himself or herself.

17 (e) Any agency that is required to issue a security breach  
18 notification pursuant to this section to more than 500 California  
19 residents as a result of a single breach of the security system shall  
20 electronically submit a single sample copy of that security breach  
21 notification, excluding any personally identifiable information, to  
22 the Attorney General. A single sample copy of a security breach  
23 notification shall not be deemed to be within subdivision (f) of  
24 Section 6254 of the Government Code.

25 (f) For purposes of this section, "breach of the security of the  
26 system" means unauthorized acquisition of computerized data that  
27 compromises the security, confidentiality, or integrity of personal  
28 information maintained by the agency. Good faith acquisition of  
29 personal information by an employee or agent of the agency for  
30 the purposes of the agency is not a breach of the security of the  
31 system, provided that the personal information is not used or  
32 subject to further unauthorized disclosure.

33 (g) For purposes of this section, "personal information" means  
34 either of the following:

35 (1) An individual's first name or first initial and last name in  
36 combination with any one or more of the following data elements,  
37 when either the name or the data elements are not encrypted:

38 (A) Social security number.

39 (B) Driver's license number or California identification card  
40 number.

1 (C) Account number, credit or debit card number, in  
2 combination with any required security code, access code, or  
3 password that would permit access to an individual's financial  
4 account.

5 (D) Medical information.

6 (E) Health insurance information.

7 (2) A user name or email address, in combination with a  
8 password or security question and answer that would permit access  
9 to an online account.

10 (h) (1) For purposes of this section, "personal information"  
11 does not include publicly available information that is lawfully  
12 made available to the general public from federal, state, or local  
13 government records.

14 (2) For purposes of this section, "medical information" means  
15 any information regarding an individual's medical history, mental  
16 or physical condition, or medical treatment or diagnosis by a health  
17 care professional.

18 (3) For purposes of this section, "health insurance information"  
19 means an individual's health insurance policy number or subscriber  
20 identification number, any unique identifier used by a health insurer  
21 to identify the individual, or any information in an individual's  
22 application and claims history, including any appeals records.

23 (i) For purposes of this section, "notice" may be provided by  
24 one of the following methods:

25 (1) Written notice.

26 (2) Electronic notice, if the notice provided is consistent with  
27 the provisions regarding electronic records and signatures set forth  
28 in Section 7001 of Title 15 of the United States Code.

29 (3) Substitute notice, if the agency demonstrates that the cost  
30 of providing notice would exceed two hundred fifty thousand  
31 dollars (\$250,000), or that the affected class of subject persons to  
32 be notified exceeds 500,000, or the agency does not have sufficient  
33 contact information. Substitute notice shall consist of all of the  
34 following:

35 (A) Email notice when the agency has an email address for the  
36 subject persons.

37 (B) Conspicuous posting, for a minimum of 30 days, of the  
38 notice on the agency's Internet Web site page, if the agency  
39 maintains one. For purposes of this subparagraph, conspicuous  
40 posting on the agency's Internet Web site means providing a link

1 to the notice on the home page or first significant page after  
2 entering the Internet Web site that is in larger type than the  
3 surrounding text, or in contrasting type, font, or color to the  
4 surrounding text of the same size, or set off from the surrounding  
5 text of the same size by symbols or other marks that call attention  
6 to the link.

7 (C) Notification to major statewide media and the Office of  
8 Information Security within the Department of Technology.

9 (4) In the case of a breach of the security of the system involving  
10 personal information defined in paragraph (2) of subdivision (g)  
11 for an online account, and no other personal information defined  
12 in paragraph (1) of subdivision (g), the agency may comply with  
13 this section by providing the security breach notification in  
14 electronic or other form that directs the person whose personal  
15 information has been breached to promptly change his or her  
16 password and security question or answer, as applicable, or to take  
17 other steps appropriate to protect the online account with the  
18 agency and all other online accounts for which the person uses the  
19 same user name or email address and password or security question  
20 or answer.

21 (5) In the case of a breach of the security of the system involving  
22 personal information defined in paragraph (2) of subdivision (g)  
23 for login credentials of an email account furnished by the agency,  
24 the agency shall not comply with this section by providing the  
25 security breach notification to that email address, but may, instead,  
26 comply with this section by providing notice by another method  
27 described in this subdivision or by clear and conspicuous notice  
28 delivered to the resident online when the resident is connected to  
29 the online account from an Internet Protocol address or online  
30 location from which the agency knows the resident customarily  
31 accesses the account.

32 (j) Notwithstanding subdivision (i), an agency that maintains  
33 its own notification procedures as part of an information security  
34 policy for the treatment of personal information and is otherwise  
35 consistent with the timing requirements of this part shall be deemed  
36 to be in compliance with the notification requirements of this  
37 section if it notifies subject persons in accordance with its policies  
38 in the event of a breach of security of the system.

39 (k) Notwithstanding the exception specified in paragraph (4) of  
40 subdivision (b) of Section 1798.3, for purposes of this section,

1 “agency” includes a local agency, as defined in subdivision (a) of  
2 Section 6252 of the Government Code.

3 *SEC. 1.1. Section 1798.29 of the Civil Code is amended to*  
4 *read:*

5 1798.29. (a) Any agency that owns or licenses computerized  
6 data that includes personal information shall disclose any breach  
7 of the security of the system following discovery or notification  
8 of the breach in the security of the data to any resident of California  
9 whose unencrypted personal information was, or is reasonably  
10 believed to have been, acquired by an unauthorized person. The  
11 disclosure shall be made in the most expedient time possible and  
12 without unreasonable delay, consistent with the legitimate needs  
13 of law enforcement, as provided in subdivision (c), or any measures  
14 necessary to determine the scope of the breach and restore the  
15 reasonable integrity of the data system.

16 (b) Any agency that maintains computerized data that includes  
17 personal information that the agency does not own shall notify the  
18 owner or licensee of the information of any breach of the security  
19 of the data immediately following discovery, if the personal  
20 information was, or is reasonably believed to have been, acquired  
21 by an unauthorized person.

22 (c) The notification required by this section may be delayed if  
23 a law enforcement agency determines that the notification will  
24 impede a criminal investigation. The notification required by this  
25 section shall be made after the law enforcement agency determines  
26 that it will not compromise the investigation.

27 (d) Any agency that is required to issue a security breach  
28 notification pursuant to this section shall meet all of the following  
29 requirements:

30 (1) The security breach notification shall be written in plain  
31 ~~language.~~ *language, shall be titled “Notice of Data Breach,” and*  
32 *shall present the information described in paragraph (2) under*  
33 *the following headings: “What Happened,” “What Information*  
34 *Was Involved,” “What We Are Doing,” “What You Can Do,” and*  
35 *“For More Information.” Additional information may be provided*  
36 *as a supplement to the notice.*

37 (A) *The format of the notice shall be designed to call attention*  
38 *to the nature and significance of the information it contains.*

39 (B) *The title and headings in the notice shall be clearly and*  
40 *conspicuously displayed.*



(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		
What You Can Do.		

1		
2	<i>Other Important Information.</i>	
3	<i>[insert other important information]</i>	
4		
5		
6		
7		
8		
9		
10		
11	<i>For More</i>	<i>Call [telephone number] or go to [Internet Web site]</i>
12	<i>Information.</i>	
13		
14		

15  
16  
17 *(E) For an electronic notice described in paragraph (2) of*  
18 *subdivision (i), use of the headings described in this paragraph*  
19 *with the information described in paragraph (2), written in plain*  
20 *language, shall be deemed to be in compliance with this*  
21 *subdivision.*

22 *(2) The security breach notification described in paragraph (1)*  
23 *shall include, at a minimum, the following information:*

24 *(A) The name and contact information of the reporting agency*  
25 *subject to this section.*

26 *(B) A list of the types of personal information that were or are*  
27 *reasonably believed to have been the subject of a breach.*

28 *(C) If the information is possible to determine at the time the*  
29 *notice is provided, then any of the following: (i) the date of the*  
30 *breach, (ii) the estimated date of the breach, or (iii) the date range*  
31 *within which the breach occurred. The notification shall also*  
32 *include the date of the notice.*

33 *(D) Whether the notification was delayed as a result of a law*  
34 *enforcement investigation, if that information is possible to*  
35 *determine at the time the notice is provided.*

36 *(E) A general description of the breach incident, if that*  
37 *information is possible to determine at the time the notice is*  
38 *provided.*

1 (F) The toll-free telephone numbers and addresses of the major  
2 credit reporting agencies, if the breach exposed a social security  
3 number or a driver's license or California identification card  
4 number.

5 (3) At the discretion of the agency, the security breach  
6 notification may also include any of the following:

7 (A) Information about what the agency has done to protect  
8 individuals whose information has been breached.

9 (B) Advice on steps that the person whose information has been  
10 breached may take to protect himself or herself.

11 ~~(4) In the case of a breach of the security of the system involving~~  
12 ~~personal information defined in paragraph (2) of subdivision (g)~~  
13 ~~for an online account, and no other personal information defined~~  
14 ~~in paragraph (1) of subdivision (g), the agency may comply with~~  
15 ~~this section by providing the security breach notification in~~  
16 ~~electronic or other form that directs the person whose personal~~  
17 ~~information has been breached to promptly change his or her~~  
18 ~~password and security question or answer, as applicable, or to take~~  
19 ~~other steps appropriate to protect the online account with the~~  
20 ~~agency and all other online accounts for which the person uses the~~  
21 ~~same user name or email address and password or security question~~  
22 ~~or answer.~~

23 ~~(5) In the case of a breach of the security of the system involving~~  
24 ~~personal information defined in paragraph (2) of subdivision (g)~~  
25 ~~for login credentials of an email account furnished by the agency,~~  
26 ~~the agency shall not comply with this section by providing the~~  
27 ~~security breach notification to that email address, but may, instead,~~  
28 ~~comply with this section by providing notice by another method~~  
29 ~~described in subdivision (i) or by clear and conspicuous notice~~  
30 ~~delivered to the resident online when the resident is connected to~~  
31 ~~the online account from an Internet Protocol address or online~~  
32 ~~location from which the agency knows the resident customarily~~  
33 ~~accesses the account.~~

34 (e) Any agency that is required to issue a security breach  
35 notification pursuant to this section to more than 500 California  
36 residents as a result of a single breach of the security system shall  
37 electronically submit a single sample copy of that security breach  
38 notification, excluding any personally identifiable information, to  
39 the Attorney General. A single sample copy of a security breach

1 notification shall not be deemed to be within subdivision (f) of  
2 Section 6254 of the Government Code.

3 (f) For purposes of this section, “breach of the security of the  
4 system” means unauthorized acquisition of computerized data that  
5 compromises the security, confidentiality, or integrity of personal  
6 information maintained by the agency. Good faith acquisition of  
7 personal information by an employee or agent of the agency for  
8 the purposes of the agency is not a breach of the security of the  
9 system, provided that the personal information is not used or  
10 subject to further unauthorized disclosure.

11 (g) For purposes of this section, “personal information” means  
12 either of the following:

13 (1) An individual’s first name or first initial and last name in  
14 combination with any one or more of the following data elements,  
15 when either the name or the data elements are not encrypted:

16 (A) Social security number.

17 (B) Driver’s license number or California identification card  
18 number.

19 (C) Account number, credit or debit card number, in  
20 combination with any required security code, access code, or  
21 password that would permit access to an individual’s financial  
22 account.

23 (D) Medical information.

24 (E) Health insurance information.

25 (F) *Information or data collected through the use or operation*  
26 *of an automated license plate recognition system, as defined in*  
27 *Section 1798.90.5.*

28 (2) A user name or email address, in combination with a  
29 password or security question and answer that would permit access  
30 to an online account.

31 (h) (1) For purposes of this section, “personal information”  
32 does not include publicly available information that is lawfully  
33 made available to the general public from federal, state, or local  
34 government records.

35 (2) For purposes of this section, “medical information” means  
36 any information regarding an individual’s medical history, mental  
37 or physical condition, or medical treatment or diagnosis by a health  
38 care professional.

39 (3) For purposes of this section, “health insurance information”  
40 means an individual’s health insurance policy number or subscriber

1 identification number, any unique identifier used by a health insurer  
2 to identify the individual, or any information in an individual's  
3 application and claims history, including any appeals records.

4 (i) For purposes of this section, "notice" may be provided by  
5 one of the following methods:

6 (1) Written notice.

7 (2) Electronic notice, if the notice provided is consistent with  
8 the provisions regarding electronic records and signatures set forth  
9 in Section 7001 of Title 15 of the United States Code.

10 (3) Substitute notice, if the agency demonstrates that the cost  
11 of providing notice would exceed two hundred fifty thousand  
12 dollars (\$250,000), or that the affected class of subject persons to  
13 be notified exceeds 500,000, or the agency does not have sufficient  
14 contact information. Substitute notice shall consist of all of the  
15 following:

16 (A) Email notice when the agency has an email address for the  
17 subject persons.

18 (B) ~~Conspicuous posting~~ *posting, for a minimum of 30 days, of*  
19 *the notice on the agency's Internet Web site page, if the agency*  
20 *maintains one. For purposes of this subparagraph, conspicuous*  
21 *posting on the agency's Internet Web site means providing a link*  
22 *to the notice on the home page or first significant page after*  
23 *entering the Internet Web site that is in larger type than the*  
24 *surrounding text, or in contrasting type, font, or color to the*  
25 *surrounding text of the same size, or set off from the surrounding*  
26 *text of the same size by symbols or other marks that call attention*  
27 *to the link.*

28 (C) Notification to major statewide media and the Office of  
29 Information Security within the Department of Technology.

30 (4) *In the case of a breach of the security of the system involving*  
31 *personal information defined in paragraph (2) of subdivision (g)*  
32 *for an online account, and no other personal information defined*  
33 *in paragraph (1) of subdivision (g), the agency may comply with*  
34 *this section by providing the security breach notification in*  
35 *electronic or other form that directs the person whose personal*  
36 *information has been breached to promptly change his or her*  
37 *password and security question or answer, as applicable, or to*  
38 *take other steps appropriate to protect the online account with the*  
39 *agency and all other online accounts for which the person uses*

1 *the same user name or email address and password or security*  
2 *question or answer.*

3 (5) *In the case of a breach of the security of the system involving*  
4 *personal information defined in paragraph (2) of subdivision (g)*  
5 *for login credentials of an email account furnished by the agency,*  
6 *the agency shall not comply with this section by providing the*  
7 *security breach notification to that email address, but may, instead,*  
8 *comply with this section by providing notice by another method*  
9 *described in this subdivision or by clear and conspicuous notice*  
10 *delivered to the resident online when the resident is connected to*  
11 *the online account from an Internet Protocol address or online*  
12 *location from which the agency knows the resident customarily*  
13 *accesses the account.*

14 (j) Notwithstanding subdivision (i), an agency that maintains  
15 its own notification procedures as part of an information security  
16 policy for the treatment of personal information and is otherwise  
17 consistent with the timing requirements of this part shall be deemed  
18 to be in compliance with the notification requirements of this  
19 section if it notifies subject persons in accordance with its policies  
20 in the event of a breach of security of the system.

21 (k) Notwithstanding the exception specified in paragraph (4) of  
22 subdivision (b) of Section 1798.3, for purposes of this section,  
23 “agency” includes a local agency, as defined in subdivision (a) of  
24 Section 6252 of the Government Code.

25 *SEC. 1.2. Section 1798.29 of the Civil Code is amended to*  
26 *read:*

27 1798.29. (a) Any agency that owns or licenses computerized  
28 data that includes personal information shall disclose any breach  
29 of the security of the system following discovery or notification  
30 of the breach in the security of the data to any resident of California  
31 whose unencrypted personal information was, or is reasonably  
32 believed to have been, acquired by an unauthorized person. The  
33 disclosure shall be made in the most expedient time possible and  
34 without unreasonable delay, consistent with the legitimate needs  
35 of law enforcement, as provided in subdivision (c), or any measures  
36 necessary to determine the scope of the breach and restore the  
37 reasonable integrity of the data system.

38 (b) Any agency that maintains computerized data that includes  
39 personal information that the agency does not own shall notify the  
40 owner or licensee of the information of any breach of the security

of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made after the law enforcement agency determines that it will not compromise the investigation.

(d) Any agency that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language. *language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.*

(A) *The format of the notice shall be designed to call attention to the nature and significance of the information it contains.*

(B) *The title and headings in the notice shall be clearly and conspicuously displayed.*

(C) *The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.*

(D) *For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.*

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		

1 2 3 4	<i>What Happened?</i>	
5 6 7 8 9 10	<i>What Information Was Involved?</i>	
11 12 13 14 15 16	<i>What We Are Doing.</i>	
17 18 19 20 21 22 23	<i>What You Can Do.</i>	
24 25 26 27 28 29 30 31 32	<i>Other Important Information.</i> <i>[insert other important information]</i>	
33 34 35 36 37 38	<i>For More Information.</i>	<i>Call [telephone number] or go to [Internet Web site]</i>



1     (E) For an electronic notice described in paragraph (2) of  
2     subdivision (i), use of the headings described in this paragraph  
3     with the information described in paragraph (2), written in plain  
4     language, shall be deemed to be in compliance with this  
5     subdivision.

6     (2) The security breach notification described in paragraph (1)  
7     shall include, at a minimum, the following information:

8     (A) The name and contact information of the reporting agency  
9     subject to this section.

10    (B) A list of the types of personal information that were or are  
11    reasonably believed to have been the subject of a breach.

12    (C) If the information is possible to determine at the time the  
13    notice is provided, then any of the following: (i) the date of the  
14    breach, (ii) the estimated date of the breach, or (iii) the date range  
15    within which the breach occurred. The notification shall also  
16    include the date of the notice.

17    (D) Whether the notification was delayed as a result of a law  
18    enforcement investigation, if that information is possible to  
19    determine at the time the notice is provided.

20    (E) A general description of the breach incident, if that  
21    information is possible to determine at the time the notice is  
22    provided.

23    (F) The toll-free telephone numbers and addresses of the major  
24    credit reporting agencies, if the breach exposed a social security  
25    number or a driver's license or California identification card  
26    number.

27    (3) At the discretion of the agency, the security breach  
28    notification may also include any of the following:

29    (A) Information about what the agency has done to protect  
30    individuals whose information has been breached.

31    (B) Advice on steps that the person whose information has been  
32    breached may take to protect himself or herself.

33    ~~(4) In the case of a breach of the security of the system involving~~  
34    ~~personal information defined in paragraph (2) of subdivision (g)~~  
35    ~~for an online account, and no other personal information defined~~  
36    ~~in paragraph (1) of subdivision (g), the agency may comply with~~  
37    ~~this section by providing the security breach notification in~~  
38    ~~electronic or other form that directs the person whose personal~~  
39    ~~information has been breached to promptly change his or her~~  
40    ~~password and security question or answer, as applicable, or to take~~

1 other steps appropriate to protect the online account with the  
2 agency and all other online accounts for which the person uses the  
3 same user name or email address and password or security question  
4 or answer.

5 (5) ~~In the case of a breach of the security of the system involving~~  
6 ~~personal information defined in paragraph (2) of subdivision (g)~~  
7 ~~for login credentials of an email account furnished by the agency;~~  
8 ~~the agency shall not comply with this section by providing the~~  
9 ~~security breach notification to that email address, but may, instead,~~  
10 ~~comply with this section by providing notice by another method~~  
11 ~~described in subdivision (i) or by clear and conspicuous notice~~  
12 ~~delivered to the resident online when the resident is connected to~~  
13 ~~the online account from an Internet Protocol address or online~~  
14 ~~location from which the agency knows the resident customarily~~  
15 ~~accesses the account.~~

16 (e) Any agency that is required to issue a security breach  
17 notification pursuant to this section to more than 500 California  
18 residents as a result of a single breach of the security system shall  
19 electronically submit a single sample copy of that security breach  
20 notification, excluding any personally identifiable information, to  
21 the Attorney General. A single sample copy of a security breach  
22 notification shall not be deemed to be within subdivision (f) of  
23 Section 6254 of the Government Code.

24 (f) For purposes of this section, “breach of the security of the  
25 system” means unauthorized acquisition of computerized data that  
26 compromises the security, confidentiality, or integrity of personal  
27 information maintained by the agency. Good faith acquisition of  
28 personal information by an employee or agent of the agency for  
29 the purposes of the agency is not a breach of the security of the  
30 system, provided that the personal information is not used or  
31 subject to further unauthorized disclosure.

32 (g) For purposes of this section, “personal information” means  
33 either of the following:

34 (1) An individual’s first name or first initial and last name in  
35 combination with any one or more of the following data elements,  
36 when either the name or the data elements are not encrypted:

37 (A) Social security number.

38 (B) Driver’s license number or California identification card  
39 number.

1 (C) Account number, credit or debit card number, in  
2 combination with any required security code, access code, or  
3 password that would permit access to an individual's financial  
4 account.

5 (D) Medical information.

6 (E) Health insurance information.

7 (2) A user name or email address, in combination with a  
8 password or security question and answer that would permit access  
9 to an online account.

10 (h) (1) For purposes of this section, "personal information"  
11 does not include publicly available information that is lawfully  
12 made available to the general public from federal, state, or local  
13 government records.

14 (2) For purposes of this section, "medical information" means  
15 any information regarding an individual's medical history, mental  
16 or physical condition, or medical treatment or diagnosis by a health  
17 care professional.

18 (3) For purposes of this section, "health insurance information"  
19 means an individual's health insurance policy number or subscriber  
20 identification number, any unique identifier used by a health insurer  
21 to identify the individual, or any information in an individual's  
22 application and claims history, including any appeals records.

23 (4) *For purposes of this section, "encrypted" means rendered*  
24 *unusable, unreadable, or indecipherable to an unauthorized person*  
25 *through a security technology or methodology generally accepted*  
26 *in the field of information security.*

27 (i) For purposes of this section, "notice" may be provided by  
28 one of the following methods:

29 (1) Written notice.

30 (2) Electronic notice, if the notice provided is consistent with  
31 the provisions regarding electronic records and signatures set forth  
32 in Section 7001 of Title 15 of the United States Code.

33 (3) Substitute notice, if the agency demonstrates that the cost  
34 of providing notice would exceed two hundred fifty thousand  
35 dollars (\$250,000), or that the affected class of subject persons to  
36 be notified exceeds 500,000, or the agency does not have sufficient  
37 contact information. Substitute notice shall consist of all of the  
38 following:

39 (A) Email notice when the agency has an email address for the  
40 subject persons.

1 (B) ~~Conspicuous-posting~~ *posting, for a minimum of 30 days, of*  
2 *the notice on the agency's Internet Web site page, if the agency*  
3 *maintains one. For purposes of this subparagraph, conspicuous*  
4 *posting on the agency's Internet Web site means providing a link*  
5 *to the notice on the home page or first significant page after*  
6 *entering the Internet Web site that is in larger type than the*  
7 *surrounding text, or in contrasting type, font, or color to the*  
8 *surrounding text of the same size, or set off from the surrounding*  
9 *text of the same size by symbols or other marks that call attention*  
10 *to the link.*

11 (C) Notification to major statewide media and the Office of  
12 Information Security within the Department of Technology.

13 (4) *In the case of a breach of the security of the system involving*  
14 *personal information defined in paragraph (2) of subdivision (g)*  
15 *for an online account, and no other personal information defined*  
16 *in paragraph (1) of subdivision (g), the agency may comply with*  
17 *this section by providing the security breach notification in*  
18 *electronic or other form that directs the person whose personal*  
19 *information has been breached to promptly change his or her*  
20 *password and security question or answer, as applicable, or to*  
21 *take other steps appropriate to protect the online account with the*  
22 *agency and all other online accounts for which the person uses*  
23 *the same user name or email address and password or security*  
24 *question or answer.*

25 (5) *In the case of a breach of the security of the system involving*  
26 *personal information defined in paragraph (2) of subdivision (g)*  
27 *for login credentials of an email account furnished by the agency,*  
28 *the agency shall not comply with this section by providing the*  
29 *security breach notification to that email address, but may, instead,*  
30 *comply with this section by providing notice by another method*  
31 *described in this subdivision or by clear and conspicuous notice*  
32 *delivered to the resident online when the resident is connected to*  
33 *the online account from an Internet Protocol address or online*  
34 *location from which the agency knows the resident customarily*  
35 *accesses the account.*

36 (j) Notwithstanding subdivision (i), an agency that maintains  
37 its own notification procedures as part of an information security  
38 policy for the treatment of personal information and is otherwise  
39 consistent with the timing requirements of this part shall be deemed  
40 to be in compliance with the notification requirements of this

1 section if it notifies subject persons in accordance with its policies  
2 in the event of a breach of security of the system.

3 (k) Notwithstanding the exception specified in paragraph (4) of  
4 subdivision (b) of Section 1798.3, for purposes of this section,  
5 “agency” includes a local agency, as defined in subdivision (a) of  
6 Section 6252 of the Government Code.

7 *SEC. 1.3. Section 1798.29 of the Civil Code is amended to*  
8 *read:*

9 1798.29. (a) Any agency that owns or licenses computerized  
10 data that includes personal information shall disclose any breach  
11 of the security of the system following discovery or notification  
12 of the breach in the security of the data to any resident of California  
13 whose unencrypted personal information was, or is reasonably  
14 believed to have been, acquired by an unauthorized person. The  
15 disclosure shall be made in the most expedient time possible and  
16 without unreasonable delay, consistent with the legitimate needs  
17 of law enforcement, as provided in subdivision (c), or any measures  
18 necessary to determine the scope of the breach and restore the  
19 reasonable integrity of the data system.

20 (b) Any agency that maintains computerized data that includes  
21 personal information that the agency does not own shall notify the  
22 owner or licensee of the information of any breach of the security  
23 of the data immediately following discovery, if the personal  
24 information was, or is reasonably believed to have been, acquired  
25 by an unauthorized person.

26 (c) The notification required by this section may be delayed if  
27 a law enforcement agency determines that the notification will  
28 impede a criminal investigation. The notification required by this  
29 section shall be made after the law enforcement agency determines  
30 that it will not compromise the investigation.

31 (d) Any agency that is required to issue a security breach  
32 notification pursuant to this section shall meet all of the following  
33 requirements:

34 (1) The security breach notification shall be written in plain  
35 ~~language.~~ *language, shall be titled “Notice of Data Breach,” and*  
36 *shall present the information described in paragraph (2) under*  
37 *the following headings: “What Happened,” “What Information*  
38 *Was Involved,” “What We Are Doing,” “What You Can Do,” and*  
39 *“For More Information.” Additional information may be provided*  
40 *as a supplement to the notice.*

(A) The format of the notice shall be designed to call attention to the nature and significance of the information it contains.

(B) The title and headings in the notice shall be clearly and conspicuously displayed.

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (i), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		

<p><i>What You Can Do.</i></p>	
<p><i>Other Important Information.</i>  <i>[insert other important information]</i></p>	
<p><i>For More Information.</i></p>	<p><i>Call [telephone number] or go to [Internet Web site]</i></p>

(E) For an electronic notice described in paragraph (2) of subdivision (i), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting agency subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

1 (E) A general description of the breach incident, if that  
2 information is possible to determine at the time the notice is  
3 provided.

4 (F) The toll-free telephone numbers and addresses of the major  
5 credit reporting agencies, if the breach exposed a social security  
6 number or a driver's license or California identification card  
7 number.

8 (3) At the discretion of the agency, the security breach  
9 notification may also include any of the following:

10 (A) Information about what the agency has done to protect  
11 individuals whose information has been breached.

12 (B) Advice on steps that the person whose information has been  
13 breached may take to protect himself or herself.

14 ~~(4) In the case of a breach of the security of the system involving~~  
15 ~~personal information defined in paragraph (2) of subdivision (g)~~  
16 ~~for an online account, and no other personal information defined~~  
17 ~~in paragraph (1) of subdivision (g), the agency may comply with~~  
18 ~~this section by providing the security breach notification in~~  
19 ~~electronic or other form that directs the person whose personal~~  
20 ~~information has been breached to promptly change his or her~~  
21 ~~password and security question or answer, as applicable, or to take~~  
22 ~~other steps appropriate to protect the online account with the~~  
23 ~~agency and all other online accounts for which the person uses the~~  
24 ~~same user name or email address and password or security question~~  
25 ~~or answer.~~

26 ~~(5) In the case of a breach of the security of the system involving~~  
27 ~~personal information defined in paragraph (2) of subdivision (g)~~  
28 ~~for login credentials of an email account furnished by the agency,~~  
29 ~~the agency shall not comply with this section by providing the~~  
30 ~~security breach notification to that email address, but may, instead,~~  
31 ~~comply with this section by providing notice by another method~~  
32 ~~described in subdivision (i) or by clear and conspicuous notice~~  
33 ~~delivered to the resident online when the resident is connected to~~  
34 ~~the online account from an Internet Protocol address or online~~  
35 ~~location from which the agency knows the resident customarily~~  
36 ~~accesses the account.~~

37 (e) Any agency that is required to issue a security breach  
38 notification pursuant to this section to more than 500 California  
39 residents as a result of a single breach of the security system shall  
40 electronically submit a single sample copy of that security breach



1 notification, excluding any personally identifiable information, to  
2 the Attorney General. A single sample copy of a security breach  
3 notification shall not be deemed to be within subdivision (f) of  
4 Section 6254 of the Government Code.

5 (f) For purposes of this section, “breach of the security of the  
6 system” means unauthorized acquisition of computerized data that  
7 compromises the security, confidentiality, or integrity of personal  
8 information maintained by the agency. Good faith acquisition of  
9 personal information by an employee or agent of the agency for  
10 the purposes of the agency is not a breach of the security of the  
11 system, provided that the personal information is not used or  
12 subject to further unauthorized disclosure.

13 (g) For purposes of this section, “personal information” means  
14 either of the following:

15 (1) An individual’s first name or first initial and last name in  
16 combination with any one or more of the following data elements,  
17 when either the name or the data elements are not encrypted:

18 (A) Social security number.

19 (B) Driver’s license number or California identification card  
20 number.

21 (C) Account number, credit or debit card number, in  
22 combination with any required security code, access code, or  
23 password that would permit access to an individual’s financial  
24 account.

25 (D) Medical information.

26 (E) Health insurance information.

27 (F) *Information or data collected through the use or operation*  
28 *of an automated license plate recognition system, as defined in*  
29 *Section 1798.90.5.*

30 (2) A user name or email address, in combination with a  
31 password or security question and answer that would permit access  
32 to an online account.

33 (h) (1) For purposes of this section, “personal information”  
34 does not include publicly available information that is lawfully  
35 made available to the general public from federal, state, or local  
36 government records.

37 (2) For purposes of this section, “medical information” means  
38 any information regarding an individual’s medical history, mental  
39 or physical condition, or medical treatment or diagnosis by a health  
40 care professional.

(3) For purposes of this section, “health insurance information” means an individual’s health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual’s application and claims history, including any appeals records.

(4) *For purposes of this section, “encrypted” means rendered unusable, unreadable, or indecipherable to an unauthorized person through a security technology or methodology generally accepted in the field of information security.*

(i) For purposes of this section, “notice” may be provided by one of the following methods:

(1) Written notice.

(2) Electronic notice, if the notice provided is consistent with the provisions regarding electronic records and signatures set forth in Section 7001 of Title 15 of the United States Code.

(3) Substitute notice, if the agency demonstrates that the cost of providing notice would exceed two hundred fifty thousand dollars (\$250,000), or that the affected class of subject persons to be notified exceeds 500,000, or the agency does not have sufficient contact information. Substitute notice shall consist of all of the following:

(A) Email notice when the agency has an email address for the subject persons.

(B) ~~Conspicuous posting~~ *posting, for a minimum of 30 days, of the notice on the agency’s Internet Web site page, if the agency maintains one. For purposes of this subparagraph, conspicuous posting on the agency’s Internet Web site means providing a link to the notice on the home page or first significant page after entering the Internet Web site that is in larger type than the surrounding text, or in contrasting type, font, or color to the surrounding text of the same size, or set off from the surrounding text of the same size by symbols or other marks that call attention to the link.*

(C) Notification to major statewide media and the Office of Information Security within the Department of Technology.

(4) *In the case of a breach of the security of the system involving personal information defined in paragraph (2) of subdivision (g) for an online account, and no other personal information defined in paragraph (1) of subdivision (g), the agency may comply with this section by providing the security breach notification in*

1 *electronic or other form that directs the person whose personal*  
2 *information has been breached to promptly change his or her*  
3 *password and security question or answer, as applicable, or to*  
4 *take other steps appropriate to protect the online account with the*  
5 *agency and all other online accounts for which the person uses*  
6 *the same user name or email address and password or security*  
7 *question or answer.*

8 (5) *In the case of a breach of the security of the system involving*  
9 *personal information defined in paragraph (2) of subdivision (g)*  
10 *for login credentials of an email account furnished by the agency,*  
11 *the agency shall not comply with this section by providing the*  
12 *security breach notification to that email address, but may, instead,*  
13 *comply with this section by providing notice by another method*  
14 *described in this subdivision or by clear and conspicuous notice*  
15 *delivered to the resident online when the resident is connected to*  
16 *the online account from an Internet Protocol address or online*  
17 *location from which the agency knows the resident customarily*  
18 *accesses the account.*

19 (j) Notwithstanding subdivision (i), an agency that maintains  
20 its own notification procedures as part of an information security  
21 policy for the treatment of personal information and is otherwise  
22 consistent with the timing requirements of this part shall be deemed  
23 to be in compliance with the notification requirements of this  
24 section if it notifies subject persons in accordance with its policies  
25 in the event of a breach of security of the system.

26 (k) Notwithstanding the exception specified in paragraph (4) of  
27 subdivision (b) of Section 1798.3, for purposes of this section,  
28 “agency” includes a local agency, as defined in subdivision (a) of  
29 Section 6252 of the Government Code.

30 SEC. 2. Section 1798.82 of the Civil Code is amended to read:

31 1798.82. (a) A person or business that conducts business in  
32 California, and that owns or licenses computerized data that  
33 includes personal information, shall disclose a breach of the  
34 security of the system following discovery or notification of the  
35 breach in the security of the data to a resident of California whose  
36 unencrypted personal information was, or is reasonably believed  
37 to have been, acquired by an unauthorized person. The disclosure  
38 shall be made in the most expedient time possible and without  
39 unreasonable delay, consistent with the legitimate needs of law  
40 enforcement, as provided in subdivision (c), or any measures

1 necessary to determine the scope of the breach and restore the  
2 reasonable integrity of the data system.

3 (b) A person or business that maintains computerized data that  
4 includes personal information that the person or business does not  
5 own shall notify the owner or licensee of the information of the  
6 breach of the security of the data immediately following discovery,  
7 if the personal information was, or is reasonably believed to have  
8 been, acquired by an unauthorized person.

9 (c) The notification required by this section may be delayed if  
10 a law enforcement agency determines that the notification will  
11 impede a criminal investigation. The notification required by this  
12 section shall be made promptly after the law enforcement agency  
13 determines that it will not compromise the investigation.

14 (d) A person or business that is required to issue a security  
15 breach notification pursuant to this section shall meet all of the  
16 following requirements:

17 (1) The security breach notification shall be written in plain  
18 language, shall be titled “Notice of Data Breach,” and shall present  
19 the information described in paragraph (2) under the following  
20 headings: “What Happened,” “What Information Was Involved,”  
21 “What We Are Doing,” “What You Can Do,” and “For More  
22 Information.” Additional information may be provided as a  
23 supplement to the notice.

24 (A) The format of the notice shall be designed to call attention  
25 to the nature and significance of the information it contains.

26 (B) The title and headings in the notice shall be clearly and  
27 conspicuously displayed.

28 (C) The text of the notice and any other notice provided pursuant  
29 to this section shall be no smaller than 10-point type.

30 (D) For a written notice described in paragraph (1) of  
31 subdivision (j), use of the model security breach notification form  
32 prescribed below or use of the headings described in this paragraph  
33 with the information described in paragraph (2), written in plain  
34 language, shall be deemed to be in compliance with this  
35 subdivision.

36  
37  
38 [NAME OF INSTITUTION / LOGO]

Date: [insert date]  
39

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38

NOTICE OF DATA BREACH	
What Happened?	
What Information Was Involved?	
What We Are Doing.	
What You Can Do.	
Other Important Information. [insert other important information]	
	Call [telephone number] or go to [Internet Web site]

For More Information.	
--------------------------	--

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security number or a driver's license or California identification card number.

(G) If the person or business providing the notification was the source of the breach, an offer to provide appropriate identity theft prevention and mitigation services, if any, shall be provided at no cost to the affected person for not less than 12 months along with all information necessary to take advantage of the offer to any person whose information was or may have been breached if the breach exposed or may have exposed personal information defined in subparagraphs (A) and (B) of paragraph (1) of subdivision (h).

1 (3) At the discretion of the person or business, the security  
2 breach notification may also include any of the following:

3 (A) Information about what the person or business has done to  
4 protect individuals whose information has been breached.

5 (B) Advice on steps that the person whose information has been  
6 breached may take to protect himself or herself.

7 (e) A covered entity under the federal Health Insurance  
8 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d  
9 et seq.) will be deemed to have complied with the notice  
10 requirements in subdivision (d) if it has complied completely with  
11 Section 13402(f) of the federal Health Information Technology  
12 for Economic and Clinical Health Act (Public Law 111-5).  
13 However, nothing in this subdivision shall be construed to exempt  
14 a covered entity from any other provision of this section.

15 (f) A person or business that is required to issue a security breach  
16 notification pursuant to this section to more than 500 California  
17 residents as a result of a single breach of the security system shall  
18 electronically submit a single sample copy of that security breach  
19 notification, excluding any personally identifiable information, to  
20 the Attorney General. A single sample copy of a security breach  
21 notification shall not be deemed to be within subdivision (f) of  
22 Section 6254 of the Government Code.

23 (g) For purposes of this section, “breach of the security of the  
24 system” means unauthorized acquisition of computerized data that  
25 compromises the security, confidentiality, or integrity of personal  
26 information maintained by the person or business. Good faith  
27 acquisition of personal information by an employee or agent of  
28 the person or business for the purposes of the person or business  
29 is not a breach of the security of the system, provided that the  
30 personal information is not used or subject to further unauthorized  
31 disclosure.

32 (h) For purposes of this section, “personal information” means  
33 either of the following:

34 (1) An individual’s first name or first initial and last name in  
35 combination with any one or more of the following data elements,  
36 when either the name or the data elements are not encrypted:

37 (A) Social security number.

38 (B) Driver’s license number or California identification card  
39 number.

1 (C) Account number, credit or debit card number, in  
2 combination with any required security code, access code, or  
3 password that would permit access to an individual's financial  
4 account.

5 (D) Medical information.

6 (E) Health insurance information.

7 (2) A user name or email address, in combination with a  
8 password or security question and answer that would permit access  
9 to an online account.

10 (i) (1) For purposes of this section, "personal information" does  
11 not include publicly available information that is lawfully made  
12 available to the general public from federal, state, or local  
13 government records.

14 (2) For purposes of this section, "medical information" means  
15 any information regarding an individual's medical history, mental  
16 or physical condition, or medical treatment or diagnosis by a health  
17 care professional.

18 (3) For purposes of this section, "health insurance information"  
19 means an individual's health insurance policy number or subscriber  
20 identification number, any unique identifier used by a health insurer  
21 to identify the individual, or any information in an individual's  
22 application and claims history, including any appeals records.

23 (j) For purposes of this section, "notice" may be provided by  
24 one of the following methods:

25 (1) Written notice.

26 (2) Electronic notice, if the notice provided is consistent with  
27 the provisions regarding electronic records and signatures set forth  
28 in Section 7001 of Title 15 of the United States Code.

29 (3) Substitute notice, if the person or business demonstrates that  
30 the cost of providing notice would exceed two hundred fifty  
31 thousand dollars (\$250,000), or that the affected class of subject  
32 persons to be notified exceeds 500,000, or the person or business  
33 does not have sufficient contact information. Substitute notice  
34 shall consist of all of the following:

35 (A) Email notice when the person or business has an email  
36 address for the subject persons.

37 (B) Conspicuous posting, for a minimum of 30 days, of the  
38 notice on the Internet Web site page of the person or business, if  
39 the person or business maintains one. For purposes of this  
40 subparagraph, conspicuous posting on the person's or business'



1 Internet Web site means providing a link to the notice on the home  
2 page or first significant page after entering the Internet Web site  
3 that is in larger type than the surrounding text, or in contrasting  
4 type, font, or color to the surrounding text of the same size, or set  
5 off from the surrounding text of the same size by symbols or other  
6 marks that call attention to the link.

7 (C) Notification to major statewide media.

8 (4) In the case of a breach of the security of the system involving  
9 personal information defined in paragraph (2) of subdivision (h)  
10 for an online account, and no other personal information defined  
11 in paragraph (1) of subdivision (h), the person or business may  
12 comply with this section by providing the security breach  
13 notification in electronic or other form that directs the person whose  
14 personal information has been breached promptly to change his  
15 or her password and security question or answer, as applicable, or  
16 to take other steps appropriate to protect the online account with  
17 the person or business and all other online accounts for which the  
18 person whose personal information has been breached uses the  
19 same user name or email address and password or security question  
20 or answer.

21 (5) In the case of a breach of the security of the system involving  
22 personal information defined in paragraph (2) of subdivision (h)  
23 for login credentials of an email account furnished by the person  
24 or business, the person or business shall not comply with this  
25 section by providing the security breach notification to that email  
26 address, but may, instead, comply with this section by providing  
27 notice by another method described in this subdivision or by clear  
28 and conspicuous notice delivered to the resident online when the  
29 resident is connected to the online account from an Internet  
30 Protocol address or online location from which the person or  
31 business knows the resident customarily accesses the account.

32 (k) Notwithstanding subdivision (j), a person or business that  
33 maintains its own notification procedures as part of an information  
34 security policy for the treatment of personal information and is  
35 otherwise consistent with the timing requirements of this part, shall  
36 be deemed to be in compliance with the notification requirements  
37 of this section if the person or business notifies subject persons in  
38 accordance with its policies in the event of a breach of security of  
39 the system.

1     *SEC. 2.1. Section 1798.82 of the Civil Code is amended to*  
2     *read:*

3     1798.82. (a) A person or business that conducts business in  
4     California, and that owns or licenses computerized data that  
5     includes personal information, shall disclose a breach of the  
6     security of the system following discovery or notification of the  
7     breach in the security of the data to a resident of California whose  
8     unencrypted personal information was, or is reasonably believed  
9     to have been, acquired by an unauthorized person. The disclosure  
10    shall be made in the most expedient time possible and without  
11    unreasonable delay, consistent with the legitimate needs of law  
12    enforcement, as provided in subdivision (c), or any measures  
13    necessary to determine the scope of the breach and restore the  
14    reasonable integrity of the data system.

15    (b) A person or business that maintains computerized data that  
16    includes personal information that the person or business does not  
17    own shall notify the owner or licensee of the information of the  
18    breach of the security of the data immediately following discovery,  
19    if the personal information was, or is reasonably believed to have  
20    been, acquired by an unauthorized person.

21    (c) The notification required by this section may be delayed if  
22    a law enforcement agency determines that the notification will  
23    impede a criminal investigation. The notification required by this  
24    section shall be made promptly after the law enforcement agency  
25    determines that it will not compromise the investigation.

26    (d) A person or business that is required to issue a security  
27    breach notification pursuant to this section shall meet all of the  
28    following requirements:

29    (1) The security breach notification shall be written in plain  
30    ~~language.~~ *language, shall be titled "Notice of Data Breach," and*  
31    *shall present the information described in paragraph (2) under*  
32    *the following headings: "What Happened," "What Information*  
33    *Was Involved," "What We Are Doing," "What You Can Do," and*  
34    *"For More Information." Additional information may be provided*  
35    *as a supplement to the notice.*

36    (A) *The format of the notice shall be designed to call attention*  
37    *to the nature and significance of the information it contains.*

38    (B) *The title and headings in the notice shall be clearly and*  
39    *conspicuously displayed.*

(C) The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.

(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		
What You Can Do.		

1		
2	<i>Other Important Information.</i>	
3	<i>[insert other important information]</i>	
4		
5		
6		
7		
8		
9		
10		
11	<i>For More</i>	<i>Call [telephone number] or go to [Internet Web site]</i>
12	<i>Information.</i>	
13		
14		

15  
16  
17 *(E) For an electronic notice described in paragraph (2) of*  
18 *subdivision (j), use of the headings described in this paragraph*  
19 *with the information described in paragraph (2), written in plain*  
20 *language, shall be deemed to be in compliance with this*  
21 *subdivision.*

22 *(2) The security breach notification described in paragraph (1)*  
23 *shall include, at a minimum, the following information:*

24 *(A) The name and contact information of the reporting person*  
25 *or business subject to this section.*

26 *(B) A list of the types of personal information that were or are*  
27 *reasonably believed to have been the subject of a breach.*

28 *(C) If the information is possible to determine at the time the*  
29 *notice is provided, then any of the following: (i) the date of the*  
30 *breach, (ii) the estimated date of the breach, or (iii) the date range*  
31 *within which the breach occurred. The notification shall also*  
32 *include the date of the notice.*

33 *(D) Whether notification was delayed as a result of a law*  
34 *enforcement investigation, if that information is possible to*  
35 *determine at the time the notice is provided.*

36 *(E) A general description of the breach incident, if that*  
37 *information is possible to determine at the time the notice is*  
38 *provided.*

1 (F) The toll-free telephone numbers and addresses of the major  
2 credit reporting agencies if the breach exposed a social security  
3 number or a driver's license or California identification card  
4 number.

5 (G) If the person or business providing the notification was the  
6 source of the breach, an offer to provide appropriate identity theft  
7 prevention and mitigation services, if any, shall be provided at no  
8 cost to the affected person for not less than 12~~months~~, *months*  
9 along with all information necessary to take advantage of the offer  
10 to any person whose information was or may have been breached  
11 if the breach exposed or may have exposed personal information  
12 defined in subparagraphs (A) and (B) of paragraph (1) of  
13 subdivision (h).

14 (3) At the discretion of the person or business, the security  
15 breach notification may also include any of the following:

16 (A) Information about what the person or business has done to  
17 protect individuals whose information has been breached.

18 (B) Advice on steps that the person whose information has been  
19 breached may take to protect himself or herself.

20 ~~(4) In the case of a breach of the security of the system involving~~  
21 ~~personal information defined in paragraph (2) of subdivision (h)~~  
22 ~~for an online account, and no other personal information defined~~  
23 ~~in paragraph (1) of subdivision (h), the person or business may~~  
24 ~~comply with this section by providing the security breach~~  
25 ~~notification in electronic or other form that directs the person whose~~  
26 ~~personal information has been breached promptly to change his~~  
27 ~~or her password and security question or answer, as applicable, or~~  
28 ~~to take other steps appropriate to protect the online account with~~  
29 ~~the person or business and all other online accounts for which the~~  
30 ~~person whose personal information has been breached uses the~~  
31 ~~same user name or email address and password or security question~~  
32 ~~or answer.~~

33 ~~(5) In the case of a breach of the security of the system involving~~  
34 ~~personal information defined in paragraph (2) of subdivision (h)~~  
35 ~~for login credentials of an email account furnished by the person~~  
36 ~~or business, the person or business shall not comply with this~~  
37 ~~section by providing the security breach notification to that email~~  
38 ~~address, but may, instead, comply with this section by providing~~  
39 ~~notice by another method described in subdivision (j) or by clear~~  
40 ~~and conspicuous notice delivered to the resident online when the~~

~~1 resident is connected to the online account from an Internet  
2 Protocol address or online location from which the person or  
3 business knows the resident customarily accesses the account.~~

(e) A covered entity under the federal Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d et seq.) will be deemed to have complied with the notice requirements in subdivision (d) if it has complied completely with Section 13402(f) of the federal Health Information Technology for Economic and Clinical Health Act (Public Law 111-5). However, nothing in this subdivision shall be construed to exempt a covered entity from any other provision of this section.

(f) A person or business that is required to issue a security breach notification pursuant to this section to more than 500 California residents as a result of a single breach of the security system shall electronically submit a single sample copy of that security breach notification, excluding any personally identifiable information, to the Attorney General. A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code.

(g) For purposes of this section, “breach of the security of the system” means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the person or business. Good faith acquisition of personal information by an employee or agent of the person or business for the purposes of the person or business is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.

(h) For purposes of this section, “personal information” means either of the following:

(1) An individual’s first name or first initial and last name in combination with any one or more of the following data elements, when either the name or the data elements are not encrypted:

(A) Social security number.

(B) Driver’s license number or California identification card number.

(C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual’s financial account.

1 (D) Medical information.

2 (E) Health insurance information.

3 (F) *Information or data collected through the use or operation*  
4 *of an automated license plate recognition system, as defined in*  
5 *Section 1798.90.5.*

6 (2) A user name or email address, in combination with a  
7 password or security question and answer that would permit access  
8 to an online account.

9 (i) (1) For purposes of this section, “personal information” does  
10 not include publicly available information that is lawfully made  
11 available to the general public from federal, state, or local  
12 government records.

13 (2) For purposes of this section, “medical information” means  
14 any information regarding an individual’s medical history, mental  
15 or physical condition, or medical treatment or diagnosis by a health  
16 care professional.

17 (3) For purposes of this section, “health insurance information”  
18 means an individual’s health insurance policy number or subscriber  
19 identification number, any unique identifier used by a health insurer  
20 to identify the individual, or any information in an individual’s  
21 application and claims history, including any appeals records.

22 (j) For purposes of this section, “notice” may be provided by  
23 one of the following methods:

24 (1) Written notice.

25 (2) Electronic notice, if the notice provided is consistent with  
26 the provisions regarding electronic records and signatures set forth  
27 in Section 7001 of Title 15 of the United States Code.

28 (3) Substitute notice, if the person or business demonstrates that  
29 the cost of providing notice would exceed two hundred fifty  
30 thousand dollars (\$250,000), or that the affected class of subject  
31 persons to be notified exceeds 500,000, or the person or business  
32 does not have sufficient contact information. Substitute notice  
33 shall consist of all of the following:

34 (A) Email notice when the person or business has an email  
35 address for the subject persons.

36 (B) ~~Conspicuous posting~~ *posting, for a minimum of 30 days, of*  
37 *the notice on the Internet Web site page of the person or business,*  
38 *if the person or business maintains one. For purposes of this*  
39 *subparagraph, conspicuous posting on the person’s or business’s*  
40 *Internet Web site means providing a link to the notice on the home*

1 *page or first significant page after entering the Internet Web site*  
2 *that is in larger type than the surrounding text, or in contrasting*  
3 *type, font, or color to the surrounding text of the same size, or set*  
4 *off from the surrounding text of the same size by symbols or other*  
5 *marks that call attention to the link.*

6 (C) Notification to major statewide media.

7 (4) *In the case of a breach of the security of the system involving*  
8 *personal information defined in paragraph (2) of subdivision (h)*  
9 *for an online account, and no other personal information defined*  
10 *in paragraph (1) of subdivision (h), the person or business may*  
11 *comply with this section by providing the security breach*  
12 *notification in electronic or other form that directs the person*  
13 *whose personal information has been breached promptly to change*  
14 *his or her password and security question or answer, as applicable,*  
15 *or to take other steps appropriate to protect the online account*  
16 *with the person or business and all other online accounts for which*  
17 *the person whose personal information has been breached uses*  
18 *the same user name or email address and password or security*  
19 *question or answer.*

20 (5) *In the case of a breach of the security of the system involving*  
21 *personal information defined in paragraph (2) of subdivision (h)*  
22 *for login credentials of an email account furnished by the person*  
23 *or business, the person or business shall not comply with this*  
24 *section by providing the security breach notification to that email*  
25 *address, but may, instead, comply with this section by providing*  
26 *notice by another method described in this subdivision or by clear*  
27 *and conspicuous notice delivered to the resident online when the*  
28 *resident is connected to the online account from an Internet*  
29 *Protocol address or online location from which the person or*  
30 *business knows the resident customarily accesses the account.*

31 (k) Notwithstanding subdivision (j), a person or business that  
32 maintains its own notification procedures as part of an information  
33 security policy for the treatment of personal information and is  
34 otherwise consistent with the timing requirements of this part, shall  
35 be deemed to be in compliance with the notification requirements  
36 of this section if the person or business notifies subject persons in  
37 accordance with its policies in the event of a breach of security of  
38 the system.

39 SEC. 2.2. *Section 1798.82 of the Civil Code is amended to*  
40 *read:*



1798.82. (a) A person or business that conducts business in California, and that owns or licenses computerized data that includes personal information, shall disclose a breach of the security of the system following discovery or notification of the breach in the security of the data to a resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person. The disclosure shall be made in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement, as provided in subdivision (c), or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.

(b) A person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of the breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person.

(c) The notification required by this section may be delayed if a law enforcement agency determines that the notification will impede a criminal investigation. The notification required by this section shall be made promptly after the law enforcement agency determines that it will not compromise the investigation.

(d) A person or business that is required to issue a security breach notification pursuant to this section shall meet all of the following requirements:

(1) The security breach notification shall be written in plain language. ~~language.~~ *language, shall be titled "Notice of Data Breach," and shall present the information described in paragraph (2) under the following headings: "What Happened," "What Information Was Involved," "What We Are Doing," "What You Can Do," and "For More Information." Additional information may be provided as a supplement to the notice.*

(A) *The format of the notice shall be designed to call attention to the nature and significance of the information it contains.*

(B) *The title and headings in the notice shall be clearly and conspicuously displayed.*

(C) *The text of the notice and any other notice provided pursuant to this section shall be no smaller than 10-point type.*

1 (D) For a written notice described in paragraph (1) of  
2 subdivision (j), use of the model security breach notification form  
3 prescribed below or use of the headings described in this  
4 paragraph with the information described in paragraph (2), written  
5 in plain language, shall be deemed to be in compliance with this  
6 subdivision.

7

8

9 [NAME OF INSTITUTION / LOGO]		Date: [insert date]
11		
12 NOTICE OF DATA BREACH		
14 What Happened?		
22 What Information 23 Was Involved?		
28 What We Are 29 Doing.		
34 What You Can 35 Do.		
39 Other Important Information.		

[insert other important information]	
For More Information.	Call [telephone number] or go to [Internet Web site]

(E) For an electronic notice described in paragraph (2) of subdivision (j), use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

(2) The security breach notification described in paragraph (1) shall include, at a minimum, the following information:

(A) The name and contact information of the reporting person or business subject to this section.

(B) A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.

(C) If the information is possible to determine at the time the notice is provided, then any of the following: (i) the date of the breach, (ii) the estimated date of the breach, or (iii) the date range within which the breach occurred. The notification shall also include the date of the notice.

(D) Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided.

(E) A general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(F) The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a social security

1 number or a driver's license or California identification card  
2 number.

3 (G) If the person or business providing the notification was the  
4 source of the breach, an offer to provide appropriate identity theft  
5 prevention and mitigation services, if any, shall be provided at no  
6 cost to the affected person for not less than 12~~months~~, *months*  
7 along with all information necessary to take advantage of the offer  
8 to any person whose information was or may have been breached  
9 if the breach exposed or may have exposed personal information  
10 defined in subparagraphs (A) and (B) of paragraph (1) of  
11 subdivision (h).

12 (3) At the discretion of the person or business, the security  
13 breach notification may also include any of the following:

14 (A) Information about what the person or business has done to  
15 protect individuals whose information has been breached.

16 (B) Advice on steps that the person whose information has been  
17 breached may take to protect himself or herself.

18 ~~(4) In the case of a breach of the security of the system involving~~  
19 ~~personal information defined in paragraph (2) of subdivision (h)~~  
20 ~~for an online account, and no other personal information defined~~  
21 ~~in paragraph (1) of subdivision (h), the person or business may~~  
22 ~~comply with this section by providing the security breach~~  
23 ~~notification in electronic or other form that directs the person whose~~  
24 ~~personal information has been breached promptly to change his~~  
25 ~~or her password and security question or answer, as applicable, or~~  
26 ~~to take other steps appropriate to protect the online account with~~  
27 ~~the person or business and all other online accounts for which the~~  
28 ~~person whose personal information has been breached uses the~~  
29 ~~same user name or email address and password or security question~~  
30 ~~or answer.~~

31 ~~(5) In the case of a breach of the security of the system involving~~  
32 ~~personal information defined in paragraph (2) of subdivision (h)~~  
33 ~~for login credentials of an email account furnished by the person~~  
34 ~~or business, the person or business shall not comply with this~~  
35 ~~section by providing the security breach notification to that email~~  
36 ~~address, but may, instead, comply with this section by providing~~  
37 ~~notice by another method described in subdivision (j) or by clear~~  
38 ~~and conspicuous notice delivered to the resident online when the~~  
39 ~~resident is connected to the online account from an Internet~~

1 ~~Protocol address or online location from which the person or~~  
2 ~~business knows the resident customarily accesses the account.~~

3 (e) A covered entity under the federal Health Insurance  
4 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d  
5 et seq.) will be deemed to have complied with the notice  
6 requirements in subdivision (d) if it has complied completely with  
7 Section 13402(f) of the federal Health Information Technology  
8 for Economic and Clinical Health Act (Public Law 111-5).  
9 However, nothing in this subdivision shall be construed to exempt  
10 a covered entity from any other provision of this section.

11 (f) A person or business that is required to issue a security breach  
12 notification pursuant to this section to more than 500 California  
13 residents as a result of a single breach of the security system shall  
14 electronically submit a single sample copy of that security breach  
15 notification, excluding any personally identifiable information, to  
16 the Attorney General. A single sample copy of a security breach  
17 notification shall not be deemed to be within subdivision (f) of  
18 Section 6254 of the Government Code.

19 (g) For purposes of this section, “breach of the security of the  
20 system” means unauthorized acquisition of computerized data that  
21 compromises the security, confidentiality, or integrity of personal  
22 information maintained by the person or business. Good faith  
23 acquisition of personal information by an employee or agent of  
24 the person or business for the purposes of the person or business  
25 is not a breach of the security of the system, provided that the  
26 personal information is not used or subject to further unauthorized  
27 disclosure.

28 (h) For purposes of this section, “personal information” means  
29 either of the following:

30 (1) An individual’s first name or first initial and last name in  
31 combination with any one or more of the following data elements,  
32 when either the name or the data elements are not encrypted:

33 (A) Social security number.

34 (B) Driver’s license number or California identification card  
35 number.

36 (C) Account number, credit or debit card number, in  
37 combination with any required security code, access code, or  
38 password that would permit access to an individual’s financial  
39 account.

40 (D) Medical information.

1 (E) Health insurance information.

2 (2) A user name or email address, in combination with a  
3 password or security question and answer that would permit access  
4 to an online account.

5 (i) (1) For purposes of this section, “personal information” does  
6 not include publicly available information that is lawfully made  
7 available to the general public from federal, state, or local  
8 government records.

9 (2) For purposes of this section, “medical information” means  
10 any information regarding an individual’s medical history, mental  
11 or physical condition, or medical treatment or diagnosis by a health  
12 care professional.

13 (3) For purposes of this section, “health insurance information”  
14 means an individual’s health insurance policy number or subscriber  
15 identification number, any unique identifier used by a health insurer  
16 to identify the individual, or any information in an individual’s  
17 application and claims history, including any appeals records.

18 (4) *For purposes of this section, “encrypted” means rendered*  
19 *unusable, unreadable, or indecipherable to an unauthorized person*  
20 *through a security technology or methodology generally accepted*  
21 *in the field of information security.*

22 (j) For purposes of this section, “notice” may be provided by  
23 one of the following methods:

24 (1) Written notice.

25 (2) Electronic notice, if the notice provided is consistent with  
26 the provisions regarding electronic records and signatures set forth  
27 in Section 7001 of Title 15 of the United States Code.

28 (3) Substitute notice, if the person or business demonstrates that  
29 the cost of providing notice would exceed two hundred fifty  
30 thousand dollars (\$250,000), or that the affected class of subject  
31 persons to be notified exceeds 500,000, or the person or business  
32 does not have sufficient contact information. Substitute notice  
33 shall consist of all of the following:

34 (A) Email notice when the person or business has an email  
35 address for the subject persons.

36 (B) ~~Conspicuous posting~~ *posting, for a minimum of 30 days, of*  
37 *the notice on the Internet Web site page of the person or business,*  
38 *if the person or business maintains one. For purposes of this*  
39 *subparagraph, conspicuous posting on the person’s or business’s*  
40 *Internet Web site means providing a link to the notice on the home*

1 *page or first significant page after entering the Internet Web site*  
2 *that is in larger type than the surrounding text, or in contrasting*  
3 *type, font, or color to the surrounding text of the same size, or set*  
4 *off from the surrounding text of the same size by symbols or other*  
5 *marks that call attention to the link.*

6 (C) Notification to major statewide media.

7 (4) *In the case of a breach of the security of the system involving*  
8 *personal information defined in paragraph (2) of subdivision (h)*  
9 *for an online account, and no other personal information defined*  
10 *in paragraph (1) of subdivision (h), the person or business may*  
11 *comply with this section by providing the security breach*  
12 *notification in electronic or other form that directs the person*  
13 *whose personal information has been breached promptly to change*  
14 *his or her password and security question or answer, as applicable,*  
15 *or to take other steps appropriate to protect the online account*  
16 *with the person or business and all other online accounts for which*  
17 *the person whose personal information has been breached uses*  
18 *the same user name or email address and password or security*  
19 *question or answer.*

20 (5) *In the case of a breach of the security of the system involving*  
21 *personal information defined in paragraph (2) of subdivision (h)*  
22 *for login credentials of an email account furnished by the person*  
23 *or business, the person or business shall not comply with this*  
24 *section by providing the security breach notification to that email*  
25 *address, but may, instead, comply with this section by providing*  
26 *notice by another method described in this subdivision or by clear*  
27 *and conspicuous notice delivered to the resident online when the*  
28 *resident is connected to the online account from an Internet*  
29 *Protocol address or online location from which the person or*  
30 *business knows the resident customarily accesses the account.*

31 (k) Notwithstanding subdivision (j), a person or business that  
32 maintains its own notification procedures as part of an information  
33 security policy for the treatment of personal information and is  
34 otherwise consistent with the timing requirements of this part, shall  
35 be deemed to be in compliance with the notification requirements  
36 of this section if the person or business notifies subject persons in  
37 accordance with its policies in the event of a breach of security of  
38 the system.

39 SEC. 2.3. *Section 1798.82 of the Civil Code is amended to*  
40 *read:*

1 1798.82. (a) A person or business that conducts business in  
2 California, and that owns or licenses computerized data that  
3 includes personal information, shall disclose a breach of the  
4 security of the system following discovery or notification of the  
5 breach in the security of the data to a resident of California whose  
6 unencrypted personal information was, or is reasonably believed  
7 to have been, acquired by an unauthorized person. The disclosure  
8 shall be made in the most expedient time possible and without  
9 unreasonable delay, consistent with the legitimate needs of law  
10 enforcement, as provided in subdivision (c), or any measures  
11 necessary to determine the scope of the breach and restore the  
12 reasonable integrity of the data system.

13 (b) A person or business that maintains computerized data that  
14 includes personal information that the person or business does not  
15 own shall notify the owner or licensee of the information of the  
16 breach of the security of the data immediately following discovery,  
17 if the personal information was, or is reasonably believed to have  
18 been, acquired by an unauthorized person.

19 (c) The notification required by this section may be delayed if  
20 a law enforcement agency determines that the notification will  
21 impede a criminal investigation. The notification required by this  
22 section shall be made promptly after the law enforcement agency  
23 determines that it will not compromise the investigation.

24 (d) A person or business that is required to issue a security  
25 breach notification pursuant to this section shall meet all of the  
26 following requirements:

27 (1) The security breach notification shall be written in plain  
28 ~~language.~~ *language, shall be titled "Notice of Data Breach," and*  
29 *shall present the information described in paragraph (2) under*  
30 *the following headings: "What Happened," "What Information*  
31 *Was Involved," "What We Are Doing," "What You Can Do," and*  
32 *"For More Information." Additional information may be provided*  
33 *as a supplement to the notice.*

34 (A) *The format of the notice shall be designed to call attention*  
35 *to the nature and significance of the information it contains.*

36 (B) *The title and headings in the notice shall be clearly and*  
37 *conspicuously displayed.*

38 (C) *The text of the notice and any other notice provided pursuant*  
39 *to this section shall be no smaller than 10-point type.*



(D) For a written notice described in paragraph (1) of subdivision (j), use of the model security breach notification form prescribed below or use of the headings described in this paragraph with the information described in paragraph (2), written in plain language, shall be deemed to be in compliance with this subdivision.

[NAME OF INSTITUTION / LOGO]		Date: [insert date]
NOTICE OF DATA BREACH		
What Happened?		
What Information Was Involved?		
What We Are Doing.		
What You Can Do.		
Other Important Information.		

1	<i>[insert other important information]</i>	
2		
3		
4		
5		
6		
7		
8		
9		<i>Call [telephone number] or go to [Internet Web site]</i>
10	<i>For More</i>	
11	<i>Information.</i>	
12		
13		
14		

15     (E) For an electronic notice described in paragraph (2) of  
 16     subdivision (j), use of the headings described in this paragraph  
 17     with the information described in paragraph (2), written in plain  
 18     language, shall be deemed to be in compliance with this  
 19     subdivision.

20     (2) The security breach notification described in paragraph (1)  
 21     shall include, at a minimum, the following information:

22     (A) The name and contact information of the reporting person  
 23     or business subject to this section.

24     (B) A list of the types of personal information that were or are  
 25     reasonably believed to have been the subject of a breach.

26     (C) If the information is possible to determine at the time the  
 27     notice is provided, then any of the following: (i) the date of the  
 28     breach, (ii) the estimated date of the breach, or (iii) the date range  
 29     within which the breach occurred. The notification shall also  
 30     include the date of the notice.

31     (D) Whether notification was delayed as a result of a law  
 32     enforcement investigation, if that information is possible to  
 33     determine at the time the notice is provided.

34     (E) A general description of the breach incident, if that  
 35     information is possible to determine at the time the notice is  
 36     provided.

37     (F) The toll-free telephone numbers and addresses of the major  
 38     credit reporting agencies if the breach exposed a social security

1 number or a driver's license or California identification card  
2 number.

3 (G) If the person or business providing the notification was the  
4 source of the breach, an offer to provide appropriate identity theft  
5 prevention and mitigation services, if any, shall be provided at no  
6 cost to the affected person for not less than 12~~months~~, *months*  
7 along with all information necessary to take advantage of the offer  
8 to any person whose information was or may have been breached  
9 if the breach exposed or may have exposed personal information  
10 defined in subparagraphs (A) and (B) of paragraph (1) of  
11 subdivision (h).

12 (3) At the discretion of the person or business, the security  
13 breach notification may also include any of the following:

14 (A) Information about what the person or business has done to  
15 protect individuals whose information has been breached.

16 (B) Advice on steps that the person whose information has been  
17 breached may take to protect himself or herself.

18 ~~(4) In the case of a breach of the security of the system involving~~  
19 ~~personal information defined in paragraph (2) of subdivision (h)~~  
20 ~~for an online account, and no other personal information defined~~  
21 ~~in paragraph (1) of subdivision (h), the person or business may~~  
22 ~~comply with this section by providing the security breach~~  
23 ~~notification in electronic or other form that directs the person whose~~  
24 ~~personal information has been breached promptly to change his~~  
25 ~~or her password and security question or answer, as applicable, or~~  
26 ~~to take other steps appropriate to protect the online account with~~  
27 ~~the person or business and all other online accounts for which the~~  
28 ~~person whose personal information has been breached uses the~~  
29 ~~same user name or email address and password or security question~~  
30 ~~or answer.~~

31 ~~(5) In the case of a breach of the security of the system involving~~  
32 ~~personal information defined in paragraph (2) of subdivision (h)~~  
33 ~~for login credentials of an email account furnished by the person~~  
34 ~~or business, the person or business shall not comply with this~~  
35 ~~section by providing the security breach notification to that email~~  
36 ~~address, but may, instead, comply with this section by providing~~  
37 ~~notice by another method described in subdivision (j) or by clear~~  
38 ~~and conspicuous notice delivered to the resident online when the~~  
39 ~~resident is connected to the online account from an Internet~~

1 ~~Protocol address or online location from which the person or~~  
2 ~~business knows the resident customarily accesses the account.~~

3 (e) A covered entity under the federal Health Insurance  
4 Portability and Accountability Act of 1996 (42 U.S.C. Sec. 1320d  
5 et seq.) will be deemed to have complied with the notice  
6 requirements in subdivision (d) if it has complied completely with  
7 Section 13402(f) of the federal Health Information Technology  
8 for Economic and Clinical Health Act (Public Law 111-5).  
9 However, nothing in this subdivision shall be construed to exempt  
10 a covered entity from any other provision of this section.

11 (f) A person or business that is required to issue a security breach  
12 notification pursuant to this section to more than 500 California  
13 residents as a result of a single breach of the security system shall  
14 electronically submit a single sample copy of that security breach  
15 notification, excluding any personally identifiable information, to  
16 the Attorney General. A single sample copy of a security breach  
17 notification shall not be deemed to be within subdivision (f) of  
18 Section 6254 of the Government Code.

19 (g) For purposes of this section, “breach of the security of the  
20 system” means unauthorized acquisition of computerized data that  
21 compromises the security, confidentiality, or integrity of personal  
22 information maintained by the person or business. Good faith  
23 acquisition of personal information by an employee or agent of  
24 the person or business for the purposes of the person or business  
25 is not a breach of the security of the system, provided that the  
26 personal information is not used or subject to further unauthorized  
27 disclosure.

28 (h) For purposes of this section, “personal information” means  
29 either of the following:

30 (1) An individual’s first name or first initial and last name in  
31 combination with any one or more of the following data elements,  
32 when either the name or the data elements are not encrypted:

33 (A) Social security number.

34 (B) Driver’s license number or California identification card  
35 number.

36 (C) Account number, credit or debit card number, in  
37 combination with any required security code, access code, or  
38 password that would permit access to an individual’s financial  
39 account.

40 (D) Medical information.

1 (E) Health insurance information.

2 (F) *Information or data collected through the use or operation*  
3 *of an automated license plate recognition system, as defined in*  
4 *Section 1798.90.5.*

5 (2) A user name or email address, in combination with a  
6 password or security question and answer that would permit access  
7 to an online account.

8 (i) (1) For purposes of this section, “personal information” does  
9 not include publicly available information that is lawfully made  
10 available to the general public from federal, state, or local  
11 government records.

12 (2) For purposes of this section, “medical information” means  
13 any information regarding an individual’s medical history, mental  
14 or physical condition, or medical treatment or diagnosis by a health  
15 care professional.

16 (3) For purposes of this section, “health insurance information”  
17 means an individual’s health insurance policy number or subscriber  
18 identification number, any unique identifier used by a health insurer  
19 to identify the individual, or any information in an individual’s  
20 application and claims history, including any appeals records.

21 (4) *For purposes of this section, “encrypted” means rendered*  
22 *unusable, unreadable, or indecipherable to an unauthorized person*  
23 *through a security technology or methodology generally accepted*  
24 *in the field of information security.*

25 (j) For purposes of this section, “notice” may be provided by  
26 one of the following methods:

27 (1) Written notice.

28 (2) Electronic notice, if the notice provided is consistent with  
29 the provisions regarding electronic records and signatures set forth  
30 in Section 7001 of Title 15 of the United States Code.

31 (3) Substitute notice, if the person or business demonstrates that  
32 the cost of providing notice would exceed two hundred fifty  
33 thousand dollars (\$250,000), or that the affected class of subject  
34 persons to be notified exceeds 500,000, or the person or business  
35 does not have sufficient contact information. Substitute notice  
36 shall consist of all of the following:

37 (A) Email notice when the person or business has an email  
38 address for the subject persons.

39 (B) ~~Conspicuous posting~~ *posting, for a minimum of 30 days, of*  
40 *the notice on the Internet Web site page of the person or business,*

1 if the person or business maintains one. *For purposes of this*  
2 *subparagraph, conspicuous posting on the person's or business's*  
3 *Internet Web site means providing a link to the notice on the home*  
4 *page or first significant page after entering the Internet Web site*  
5 *that is in larger type than the surrounding text, or in contrasting*  
6 *type, font, or color to the surrounding text of the same size, or set*  
7 *off from the surrounding text of the same size by symbols or other*  
8 *marks that call attention to the link.*

9 (C) Notification to major statewide media.

10 (4) *In the case of a breach of the security of the system involving*  
11 *personal information defined in paragraph (2) of subdivision (h)*  
12 *for an online account, and no other personal information defined*  
13 *in paragraph (1) of subdivision (h), the person or business may*  
14 *comply with this section by providing the security breach*  
15 *notification in electronic or other form that directs the person*  
16 *whose personal information has been breached promptly to change*  
17 *his or her password and security question or answer, as applicable,*  
18 *or to take other steps appropriate to protect the online account*  
19 *with the person or business and all other online accounts for which*  
20 *the person whose personal information has been breached uses*  
21 *the same user name or email address and password or security*  
22 *question or answer.*

23 (5) *In the case of a breach of the security of the system involving*  
24 *personal information defined in paragraph (2) of subdivision (h)*  
25 *for login credentials of an email account furnished by the person*  
26 *or business, the person or business shall not comply with this*  
27 *section by providing the security breach notification to that email*  
28 *address, but may, instead, comply with this section by providing*  
29 *notice by another method described in this subdivision or by clear*  
30 *and conspicuous notice delivered to the resident online when the*  
31 *resident is connected to the online account from an Internet*  
32 *Protocol address or online location from which the person or*  
33 *business knows the resident customarily accesses the account.*

34 (k) Notwithstanding subdivision (j), a person or business that  
35 maintains its own notification procedures as part of an information  
36 security policy for the treatment of personal information and is  
37 otherwise consistent with the timing requirements of this part, shall  
38 be deemed to be in compliance with the notification requirements  
39 of this section if the person or business notifies subject persons in

accordance with its policies in the event of a breach of security of the system.

*SEC. 3. (a) Section 1.1 of this bill incorporates amendments to Section 1798.29 of the Civil Code proposed by both this bill and Senate Bill 34. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2016, (2) each bill amends Section 1798.29 of the Civil Code, (3) Assembly Bill 964 is not enacted or as enacted does not amend that section, and (4) this bill is enacted after Senate Bill 34, in which case Sections 1, 1.2, and 1.3 of this bill shall not become operative.*

*(b) Section 1.2 of this bill incorporates amendments to Section 1798.29 of the Civil Code proposed by both this bill and Assembly Bill 964. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2016, (2) each bill amends Section 1798.29 of the Civil Code, (3) Senate Bill 34 is not enacted or as enacted does not amend that section, and (4) this bill is enacted after Assembly Bill 964, in which case Sections 1, 1.1 and 1.3 of this bill shall not become operative.*

*(c) Section 1.3 of this bill incorporates amendments to Section 1798.29 of the Civil Code proposed by this bill, Senate Bill 34, and Assembly Bill 964. It shall only become operative if (1) all three bills are enacted and become effective on or before January 1, 2016, (2) all three bills amend Section 1798.29 of the Civil Code, and (3) this bill is enacted after Senate Bill 34 and Assembly Bill 964, in which case Sections 1, 1.1 and 1.2 of this bill shall not become operative.*

*SEC. 4. (a) Section 2.1 of this bill incorporates amendments to Section 1798.82 of the Civil Code proposed by both this bill and Senate Bill 34. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2016, (2) each bill amends Section 1798.82 of the Civil Code, (3) Assembly Bill 964 is not enacted or as enacted does not amend that section, and (4) this bill is enacted after Senate Bill 34, in which case Sections 2, 2.2, and 2.3 of this bill shall not become operative.*

*(b) Section 2.2 of this bill incorporates amendments to Section 1798.82 of the Civil Code proposed by both this bill and Assembly Bill 964. It shall only become operative if (1) both bills are enacted and become effective on or before January 1, 2016, (2) each bill*

1 amends Section 1798.82 of the Civil Code, (3) Senate Bill 34 is  
2 not enacted or as enacted does not amend that section, and (4)  
3 this bill is enacted after Assembly Bill 964, in which case Sections  
4 2, 2.1, and 2.3 of this bill shall not become operative.

5 (c) Section 2.3 of this bill incorporates amendments to Section  
6 1798.82 of the Civil Code proposed by this bill, Senate Bill 34,  
7 and Assembly Bill 964. It shall only become operative if (1) all  
8 three bills are enacted and become effective on or before January  
9 1, 2016, (2) all three bills amend Section 1798.82 of the Civil Code,  
10 and (3) this bill is enacted after Senate Bill 34 and Assembly Bill  
11 964, in which case Sections 2, 2.1, and 2.2 of this bill shall not  
12 become operative.